

# INFORMATION-PRESERVING SYSTEM, INFORMATION MOVING SYSTEM AND STORAGE MEDIUM USED FOR THEM

Patent number: JP2002101087

Publication date: 2002-04-05

Inventor: ASAHU TAKESHI; KAWASAKI IKUYA; KITAHARA JUN;  
MIZUSHIMA EIGA; OWADA TORU; TAMURA  
TAKAYUKI; TOTSUKA TAKASHI

Applicant: HITACHI LTD

Classification:

- international: H04L9/10; G06F12/14; H04L9/08

- european:

Application number: JP20000286479 20000921

Priority number(s): JP20000286479 20000921

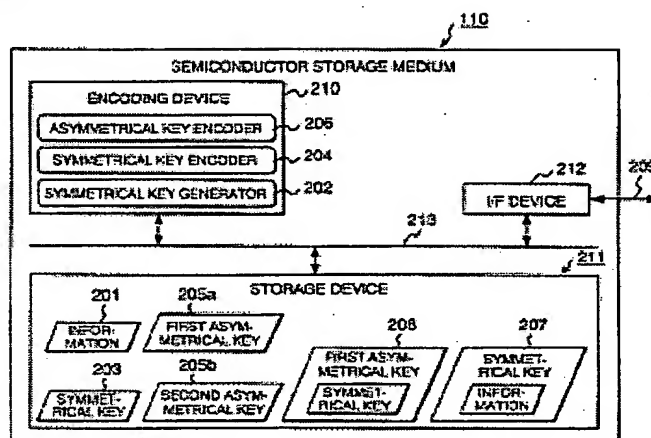
Also published as:

US2002034306 (A1)

Abstract not available for JP2002101087

Abstract of corresponding document: **US2002034306**

A storage medium and an information processing system utilizing that storage medium capable of outputting information stored on the storage medium in a format unusable by other information devices or storage mediums. A storage medium and an information processing system utilizing that storage medium further capable of transferring information stored on the storage medium rather than copying the information so that the uniqueness of the information is assured. A storage medium comprised of a storage device for storing information, information required for encryption and encrypted information, and an I/F device for inputting and outputting information, information required for coding and store encrypted information in a storage device or from an external apparatus other than the storage device, and an encoding device for coding of information and decoding of encoded information. When outputting information stored inside the storage device to outside the storage medium, information is encoded using encryption key information, and along with obtaining the encoded information and obtaining the encoded encryption key information by using another encryption information, both the encoded information and encoded encryption key information are output so that decoding the information without the storage medium is impossible



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-101087

(P2002-101087A)

(43) 公開日 平成14年4月5日 (2002.4.5)

(51) Int.Cl.<sup>7</sup>

識別記号

F I

ターマコード (参考)

H 0 4 L 9/10

G 0 6 F 12/14

3 2 0 B 5 B 0 1 7

G 0 6 F 12/14

3 2 0

3 2 0 E 5 J 1 0 4

H 0 4 L 9/00

6 2 1 A

6 0 1 C

6 0 1 E

H 0 4 L 9/08

審査請求 未請求 請求項の数 5 O L (全 14 頁)

(21) 出願番号

特願2000-286479 (P2000-286479)

(22) 出願日

平成12年9月21日 (2000.9.21)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 大和田 徹

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 北原 潤

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74) 代理人 100068504

弁理士 小川 勝男 (外2名)

最終頁に続く

(54) 【発明の名称】 情報保管システム及び情報移動システム並びにそれらに用いる記憶媒体

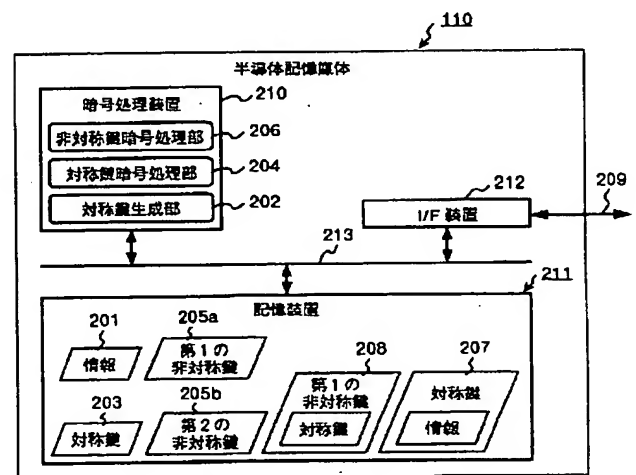
(57) 【要約】

(修正有)

【課題】 記憶媒体に格納されている情報を他の情報機器又は記憶媒体で使用することが不可能な形式で出力し、該情報を複製ではなく移動して、情報の唯一性を保証する記憶媒体及び情報処理システムを提供する。

【解決手段】 記憶媒体110は、情報、暗号化に必要な情報、及び暗号化された情報を保管する記憶装置211と保管された上記情報を記憶媒体以外の外部機器から入力し、且つ出力するI/F装置212、及び、情報に対する暗号化、復号化を行なう暗号処理装置210を備え、更に、保管した情報を記憶媒体外に出力する時に、該情報に暗号鍵情報を用いた暗号化情報を得ると共に、該情報を暗号化する際に用いた暗号鍵情報を、該暗号鍵情報とは独立の、該暗号鍵情報を暗号化する際に用いる暗号鍵情報を用いて暗号化し、暗号化暗号鍵情報を得、該暗号化情報と該暗号化暗号鍵情報を共に出力することで、該記憶媒体以外では該情報を復号化することを困難とする。

図 2



## 【特許請求の範囲】

【請求項 1】 情報、暗号処理に必要な暗号処理鍵、及び暗号化された暗号化情報を保管する記憶装置と、該記憶装置に保管された該情報、該暗号処理鍵、又は該暗号化情報の入出力を行う入力装置と、該情報に対する暗号処理、該暗号化情報に対する復号処理を行なう暗号処理装置とを備え、

該記憶装置内に保管した情報を記憶媒体外に出力する場合には、該情報を該暗号処理鍵を用いて暗号化した該暗号化情報を得ると共に、該情報を暗号化する際に用いた該暗号処理鍵を、他の暗号処理鍵を用いて暗号化した暗号化暗号処理鍵を得、該暗号化情報と該暗号化暗号処理鍵を共に出力するように構成されることを特徴とする記憶媒体。

【請求項 2】 情報、暗号処理に必要な暗号処理鍵、及び暗号化された暗号化情報を保管する記憶装置と、該記憶装置に保管された、該情報、該暗号処理鍵、又は該暗号化情報の入出力を行う入力装置と、該情報に対する暗号処理、該暗号化情報に対する復号処理を行なう暗号処理装置とを備え、

該記憶装置内に保管した情報を記憶媒体外に出力する場合には、該情報を該暗号処理鍵を用いて暗号化して該暗号化情報を得ると共に、該情報を暗号化する際に用いた該暗号処理鍵を、他の暗号処理鍵を用いて暗号化した暗号化暗号処理鍵を得、先ず、該暗号化情報のみを出力し、外部機器から該暗号化情報が入力されたことを示す信号が入力された時、該記憶装置に保管された情報を無効化した後、該暗号化暗号処理鍵を出力するように構成されることを特徴とする記憶媒体。

【請求項 3】 請求項 1 又は 2 記載の記憶媒体において、該記憶媒体の有する入力装置、該暗号処理装置及び該記憶装置が同一の半導体チップ上に構成されることを特徴とする記憶媒体。

【請求項 4】 情報、暗号処理に必要な暗号処理鍵、及び暗号化された暗号化情報を保管する記憶装置、該記憶装置に保管された、該情報、該暗号処理鍵、又は該暗号化情報の入出力を行う入力装置、該情報に対する暗号処理、該暗号化情報に対する復号処理を行なう暗号処理装置を有する記憶媒体と、

該記憶媒体と接続される外部装置と、を備え、該情報を該暗号処理鍵を用いて暗号化して得た該暗号化情報と、該情報を暗号化する際に用いた該暗号処理鍵を、他の暗号処理鍵を用いて暗号化した暗号化暗号処理鍵とを該外部装置に転送して記憶することを特徴とする情報保管システム。

【請求項 5】 情報、暗号処理に必要な暗号処理鍵、及び暗号化された暗号化情報を保管する記憶装置、該記憶装置に保管された、該情報、該暗号処理鍵、又は該暗号化情報の入出力を行う入力装置、該情報に対する暗号処理、該暗号化情報に対する復号処理を行なう暗号処理装

置を有する記憶媒体と、

該記憶媒体に記憶された情報を受信する外部装置と、を備え、

該情報を該外部装置に転送する場合には、該情報を該暗号処理鍵を用いて暗号化して得た該暗号化情報を該外部装置に転送し、該外部装置から該暗号化情報を受信したことを示す信号を受信した後、該記憶装置に保管された情報を無効化し、該暗号化暗号処理鍵を該外部装置に転送することを特徴とする情報移動システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、情報を半導体記憶媒体で流通させる場合の情報保管システム及び情報移動システム並びにこれらに用いる記憶媒体に係り、特に、付加価値の高い情報を、複製による不正使用を防ぎながら、例えば PC 向けの大容量磁気記憶装置など特に情報の複製防止機能を具備していない汎用の情報記憶媒体に保管する方法及び同情報を記憶媒体間での複製を許さずに移動する方法に関する。

## 【0002】

【従来の技術】 従来の付加価値の高い情報を、複製による不正使用を防ぎながら流通させる方式として、特開 2000-90039 号公報に記載されているようなシステムがある。図 9 を用いて同装置の動作を簡単に説明する。図 9 は従来の複製による不正使用防止システムを示すブロック図である。同システムでは、音楽サーバ 903 とクライアント 902 がインターネット 901 で接続されている。クライアント 902 において、再生装置 911 固有の ID に基づき公開鍵及び秘密鍵が作成される。公開鍵は、パーソナルコンピュータ 902 からサーバ 903 に送られ、登録される。秘密鍵は、装置 911 に保持される。クライアント 902 からサーバ 903 に対して、音楽データの配信が要求される。音楽 DB 922 から取り出された音楽データに対して、登録された公開鍵で暗号化が施される。暗号化された音楽データがクライアント 902 に送信され、再生装置 911 に保存される。再生時には、再生装置 911 に保持された秘密鍵で音楽データが復号化されながら再生される。再生装置 911 に保存された音楽データは、再生装置 911 固有の ID に基づき作成された鍵で暗号化されているため、他の再生装置では再生できない。

【0003】 又、従来の付加価値の高い情報を、記憶媒体間での複製を許さずに移動する方式として、特開平 11-259964 号公報に記載されているような装置がある。図 10 を用いて同装置の動作を簡単に説明する。図 10 は従来の情報移動システムのフローチャートである。同装置では、移動によってデータを移動先に複製すると、移動元のデータは、再生が禁止される。移動先の機器には、予め固有の識別子が設定される。ステップ 1050 で移動元機器に移動先機器が接続されると、ステ

ステップ1051で移動先機器から識別子が送信される。移動先では、ステップ1052で、予め登録された識別子管理表から送信された識別子が探され、ステップ1053でこの識別子が見つかったか、見つからなかったかを判断する。見つからなければステップ1061に移行し、移動が禁止される。ステップ1053で識別子が見つければ、ステップ1054で曲の選択が行われ、移動の指示がなされる。次に、ステップ1055で移動元でデータ管理表から移動するデータが探され、ステップ1056でフラグが調べられる。ステップ1057でフラグが「1」であれば、ステップ1061に移行して、そのデータが既に移動されたとして移動が禁止される。フラグが「0」であれば、ステップ1058で、データが移動され、ステップ1059で、データ管理表が更新される。

#### 【0004】

【発明が解決しようとする課題】従来、半導体記憶媒体に格納された情報は、他の半導体記憶媒体への複製が容易に行なえるため、情報に付加価値をつけることが困難であるという問題があった。逆に言えば、付加価値の高いデータは、簡単に複製されてしまうのを防止するために半導体記憶媒体で流通させることは行われてこなかった。これに対し、従来の付加価値の高い情報を、複製による不正使用を防ぎながら流通させる方式では、サーバ903が、付加価値の高い情報を、再生装置911固有のIDに基づき暗号化するため、通信系路上で同情報を盗聴し不正に利用することを防止することが可能である。

【0005】又、転送元機器から転送先機器に暗号化情報を渡す際、「例えば音楽データなどの高付加価値情報を、共通鍵暗号方式で暗号化して転送する。」「上記暗号化に用いた共通鍵を、公開鍵暗号方式で暗号化して転送する。」と言った二段に鍵を組み合わせた暗号化は処理速度、鍵管理の容易性から一般的である。ここで、後者の暗号化は、転送先機器で復号可能な暗号鍵を用いている（鍵の共有を行なっている）ことから、転送先機器で有価値情報を利用することが可能となっている。

【0006】又、従来の付加価値の高い情報を、記憶媒体間での複製を許さずに移動する方式では、データの複製許可／不許可フラグとデータ複製後のデータ移動元でのデータ再生禁止機能を設けることで、付加価値の高い情報の移動を実現している。しかし、同方式においては情報の移動元、移動先間の通信経路の保護が十分でなく同通信経路上の盗聴で、付加価値の高い情報の不正な取得を許してしまう可能性がある。又、一連の移動処理途上で、データ移動元、移動先に利用可能なデータが存在する時点がありデータ移動元、移動先間の通信遮断などによりデータ移動元、移動先のデータが共に利用可能となってしまう可能性がある。

【0007】本発明の目的は上記問題点を解決するため

になされたものであり、記憶媒体自体への機能追加により、同記憶媒体に格納されている情報を他の情報機器又は記憶媒体で使用することが不可能な形式で出力する（鍵を共有しない）ことが可能な記憶媒体及びそれを用いた情報処理技術を提供することにある。更に、本発明の他の目的は記憶媒体に格納されている情報を、通信経路上の盗聴による複製を防止しつつ、複製ではなく移動することで、常に情報の唯一性を保証することが可能な記憶媒体及びそれを用いた情報処理技術を提供することにある。

#### 【0008】

【課題を解決するための手段】本発明の目的を達成するために、第1の発明では、記憶媒体は、情報、暗号処理に必要な暗号処理鍵、及び暗号化された暗号化情報を保管する記憶装置と、該記憶装置に保管された該情報、該暗号処理鍵、又は該暗号化情報の入出力を行う入力装置と、該情報に対する暗号処理、該暗号化情報に対する復号処理を行なう暗号処理装置とを備え、該記憶装置内に保管した情報を記憶媒体外に出力する場合には、該情報を該暗号処理鍵を用いて暗号化した該暗号化情報を得ると共に、該情報を暗号化する際に用いた該暗号処理鍵を、他の暗号処理鍵を用いて暗号化した暗号化暗号処理鍵を得、該暗号化情報と該暗号化暗号処理鍵を共に出力するように構成される。

【0009】第2の発明では、記憶媒体は、情報、暗号処理に必要な暗号処理鍵、及び暗号化された暗号化情報を保管する記憶装置と、該記憶装置に保管された、該情報、該暗号処理鍵、又は該暗号化情報の入出力を行う入力装置と、該情報に対する暗号処理、該暗号化情報に対する復号処理を行なう暗号処理装置とを備え、該記憶装置内に保管した情報を記憶媒体外に出力する場合には、該情報を該暗号処理鍵を用いて暗号化して該暗号化情報を得ると共に、該情報を暗号化する際に用いた該暗号処理鍵を、他の暗号処理鍵を用いて暗号化した暗号化暗号処理鍵を得、先ず、該暗号化情報のみを出力し、外部機器から該暗号化情報が入力されたことを示す信号が入力された時、該記憶装置に保管された情報を無効化した後、該暗号化暗号処理鍵を出力するように構成される。

【0010】第1または第2の発明において、該記憶媒体の有する入力装置、該暗号処理装置及び該記憶装置が同一の半導体チップ上に構成される。

【0011】第3の発明では、情報保管システムは、情報、暗号処理に必要な暗号処理鍵、及び暗号化された暗号化情報を保管する記憶装置、該記憶装置に保管された、該情報、該暗号処理鍵、又は該暗号化情報の入出力を行う入力装置、該情報に対する暗号処理、該暗号化情報に対する復号処理を行なう暗号処理装置を有する記憶媒体と、該記憶媒体と接続される外部装置とを備え、該情報を該暗号処理鍵を用いて暗号化して得た該暗号化情報と、該情報を暗号化する際に用いた該暗号処理鍵を、

他の暗号処理鍵を用いて暗号化した暗号化暗号処理鍵とを該外部装置に転送して記憶する。

【0012】第4の発明では、情報移動システムは、情報、暗号処理に必要な暗号処理鍵、及び暗号化された暗号化情報を保管する記憶装置、該記憶装置に保管された、該情報、該暗号処理鍵、又は該暗号化情報の入出力を行う入力装置、該情報に対する暗号処理、該暗号化情報に対する復号処理を行なう暗号処理装置を有する記憶媒体と、該記憶媒体に記憶された情報を受信する外部装置とを備え、該情報を該外部装置に転送する場合には、該情報を該暗号処理鍵を用いて暗号化して得た該暗号化情報を該外部装置に転送し、該外部装置から該暗号化情報を受信したことを示す信号を受信した後、該記憶装置に保管された情報を無効化し、該暗号化暗号処理鍵を該外部装置に転送する。

【0013】

【発明の実施の形態】以下、本発明の実施の形態について、幾つかの実施例を用い、図を参照して説明する。図1は本発明を適用することができる情報処理システムの一実施例の概要を示すブロック図である。図に示すように、情報処理システムは、情報を生成する情報生成者および情報生成装置101と、転送手段102を介して接続された、情報配信装置103と、情報配信装置103と通信回線104で接続された、少なくとも1台の専用情報処理装置105と、少なくとも1個の半導体記憶媒体110と、少なくとも1台の情報再生装置109からなる。

【0014】専用情報処理装置105以外に、通信回線104に接続可能な、半導体記憶媒体アクセス手段107を備えた、パーソナルコンピュータ等の汎用情報処理装置106と、情報再生装置108が存在しても良い。情報は、情報生成者および情報生成装置101で生成され、情報配信装置103内に格納される。この時の情報の転送には、通信回線を用いても良いし、フロッピー（登録商標）ディスク等の磁気記憶媒体を介して、転送されても良い。情報配信装置103は、同装置に格納された情報を、専用情報処理装置105、汎用情報処理装置106、情報再生装置108からの要求に応じて、情報を加工し、または補助情報を付加し、通信回線104を介して転送する。

【0015】情報を転送された専用情報処理装置105、汎用情報処理装置106、情報再生装置108は、接続されている半導体記憶媒体110に、情報を転送する。専用情報処理装置105は、複数の情報を蓄積しておき、専用情報処理装置105で情報の加工および補助情報の付加の処理を行っても良い。汎用情報処理装置106、情報再生装置108は、情報配信装置103から転送された情報を基本的にそのまま半導体記憶媒体110に転送する。このとき、情報配信装置103と専用情報処理装置105間、専用情報処理装置105と半導体

記憶媒体110間、情報配信装置103と半導体記憶媒体110間ではそれぞれを認識し正当性を判断する情報交換を行う。

【0016】加工または補助情報を付加された配信情報を格納した半導体記憶媒体110は、情報再生装置109に接続され、情報再生装置109からの要求に応じて、格納してある情報を転送する。このとき、半導体記憶媒体110と、情報再生装置109とを認識し正当性を判断する情報交換を行う。

【0017】尚、情報生成者及び情報生成装置101が生成した情報を半導体記憶媒体110に安全に配信する方法は、本発明では特に言及せず、半導体記憶媒体110には配信された情報が格納されていることを前提とする。

【0018】以下、本発明の第1の実施例について、図2～図4、及び図8を用いて説明する。図2は本発明による記憶媒体の第1の実施例を示す構成図であり、半導体記憶媒体110は主に暗号処理装置210と記憶装置211及びI/F装置212から構成される。図において、暗号処理装置210は、非対称鍵暗号や公開鍵暗号と呼ばれる、暗号鍵と復号鍵が異なる暗号方式を用いた暗号処理を行う非対称鍵暗号処理部206と、対称鍵暗号や共通鍵暗号と呼ばれる、暗号鍵と復号鍵が同じである暗号方式を用いた暗号処理である対称鍵暗号処理204と、何らかの乱数生成処理を用いた対称鍵生成処理202などから構成される。記憶装置211は、情報201、対称鍵203、第1の非対称鍵205a、第2の非対称鍵205b、第1の非対称鍵で暗号化された対称鍵208、対称鍵で暗号化された情報207などを保管する。インターフェース装置212（以下、I/F装置と言う）は、半導体記憶媒体110と外部機器との間の情報のやり取りを制御する。データバス213は、暗号処理装置210、記憶装置211、I/F装置212間で情報、制御信号をやり取りする。また、データバス209は半導体記憶媒体110と外部機器間で情報、制御信号をやり取りする。

【0019】半導体記憶媒体110にはあらかじめ記憶媒体固有情報を記録しておく。すなわち、記憶装置211には、半導体記憶媒体110固有の第1の非対称鍵205aと第2の非対称鍵205bの2つが記憶される。固有情報を設定するには、半導体記憶媒体110を製造する段階で書き込み、半導体記憶媒体110が完成してからは容易に書き換えることが不可能な方式をとってもよいし、製造管理者など限定され、かつ情報の管理が十分に行なえる範囲にのみ公開される方式を用いて、半導体記憶媒体110の完成後に、固有情報を設定する方式をとってもよい。

【0020】この半導体記憶媒体110固有の第1、第2の非対称鍵205a、205bは非対称鍵暗号や公開鍵暗号と呼ばれる方式の鍵データである。非対称鍵暗号

や公開鍵暗号と呼ばれる暗号方式は、平文を第1の非対称鍵を暗号鍵として暗号化し暗号文を生成すると、暗号文は第2の非対称鍵を復号鍵としてのみ復号が可能となり、平文を第2の非対称鍵を暗号鍵として暗号化し暗号文を生成すると、暗号文は第1の非対称鍵を復号鍵としてのみ復号が可能となるという特徴を持つ暗号方式である。以下では、第1の非対称鍵を公開鍵、第2の非対称鍵を秘密鍵として用いる。また、207は対称鍵を用いて暗号化された情報である暗号化情報を意味し、208は非対称鍵を用いて対称鍵を暗号化された対称鍵である暗号化対称鍵を意味する。

【0021】次に、図3及び図8(a)を用いて、本実施例に掛かる半導体記憶媒体110に保管された情報201を汎用情報処理装置106及び半導体記憶媒体アクセス手段107へ情報201を転送する場合の手順を説明する。図3は本発明による情報移動システムの記憶媒体からの情報転送機能の第1の実施例を示す図であり、図8(a)、(b)は図3の情報移動システムの動作を説明するためのフローチャートであり、(a)は半導体記憶媒体110からの情報転送の動作を示し、(b)は半導体記憶媒体110への情報転送を示す。

【0022】半導体記憶媒体110に接続された汎用情報処理装置106及び半導体記憶媒体アクセス手段107による情報201の転送要求に応じて、半導体記憶媒体110は以下の動作を行う。

【0023】図2、図3および図8を参照して説明すると、ステップ202で、半導体記憶媒体110は暗号処理装置210の機能によって乱数を生成する。生成された乱数は情報201を暗号化する対称鍵203として用いられる。ステップ204aで、情報201は、暗号処理装置210の機能によって、対称鍵203を暗号鍵とした対称鍵暗号化が施され、暗号化情報207が生成される。一方、対称鍵203は、ステップ206aに示すように、暗号処理装置210の機能によって、第1の非対称鍵205aを暗号鍵として、非対称暗号化が施され、暗号化対称鍵208が生成される。

【0024】上記手順により生成された暗号化情報207及び暗号化対称鍵208は、I/F装置212の機能によって、ステップ209aで、汎用情報処理装置106及び半導体記憶媒体アクセス手段107に転送される。これによって、暗号化情報207及び暗号化対称鍵208は汎用情報処理装置106及び半導体記憶媒体アクセス手段107にバックアップ用として保管することができる。

【0025】上記手順によって汎用情報処理装置106及び半導体記憶媒体アクセス手段107に転送された暗号化情報207は、対称鍵203がないと正当に復号できない。又、暗号化対称鍵208は、第2の非対称鍵205bがないと正当に復号できない。ここで、第2の非対称鍵205bは、半導体記憶媒体110固有の鍵デー

タであり、汎用情報処理装置106及び半導体記憶媒体アクセス手段107はこれを得ることができない。従って、該汎用情報処理装置106及び半導体記憶媒体アクセス手段107は、暗号化対称鍵208を復号して情報201を利用することができない。

【0026】つまり、半導体記憶媒体110上に保管された情報201は、汎用情報処理装置106及び半導体記憶媒体アクセス手段107に転送された後、汎用情報処理装置106などの機能によってその複製を作成されることがあっても、該複製情報は汎用情報処理装置106及び半導体記憶媒体アクセス手段107上では使用不可能である、このことから、汎用情報処理装置106での情報201の無制限な複製を防ぐことが可能である。

【0027】又、転送されるべき情報201を暗号化するため用いた対称鍵203は、情報201の復号のために必須であるため、本来は半導体記憶媒体110内に転送される情報毎に管理、保管されるべきであるが、本実施例に係る半導体記憶媒体110は、対称鍵203を半導体記憶媒体110固有の第1の非対称鍵205aで暗号化された暗号化対称鍵208とし、ステップ209aで暗号化情報207と共に、半導体記憶媒体110外に転送される。このことにより、半導体記憶媒体110内で複数の対称鍵を管理、保管する必要がなくなるので、第1及び第2の非対称鍵ペア205a、205bのみ管理、保管すればよい。すなわち、鍵管理が容易となると共に複数の対称鍵データによって記憶装置211の記憶容量を占有しないという利点がある。

【0028】次に、図4及び図8(b)を用いて、図3に示した手順によって汎用情報処理装置106及び半導体記憶媒体アクセス手段107へ転送された暗号化情報207を、半導体記憶媒体110へ転送する場合の手順を説明する。

【0029】図4は本発明による情報移動システムの記録媒体への情報転送機能の第1の実施例を示す図である。半導体記憶媒体110に接続された汎用情報処理装置106及び半導体記憶媒体アクセス手段107による情報201の転送要求に応じて、半導体記憶媒体110は以下の動作を行う。半導体記憶媒体110は、ステップ209bにおいて、I/F装置212の機能によって汎用情報処理装置106及び半導体記憶媒体アクセス手段107から暗号化情報207及び暗号化対称鍵208を入力する。次に、半導体記憶媒体110は、ステップ206bで、暗号処理装置210の機能によって第2の非対称鍵205bを復号鍵として暗号化対称鍵208に非対称復号化を施し、対称鍵203を得る。更に、ステップ204bで、暗号処理装置210の機能によって上記手順で得られた対称鍵203を復号鍵として暗号化情報207に対称鍵復号化を施し、情報201を得る。

【0030】ここで、第2の非対称鍵205bは、半導体記憶媒体110固有の鍵データであることから、汎用



情報処理装置 106 及び半導体記憶媒体アクセス手段 107 に転送された暗号化情報 207 は、暗号化情報 207 の転送元となった同一の半導体記憶媒体 110 のみ復号可能である。このことから、汎用情報処理装置 106 及び半導体記憶媒体アクセス手段 107 に転送された暗号化情報 207 を転送元となった半導体記憶媒体 110 以外の半導体記憶媒体に転送して復号、使用することは不可能であり、情報 201 の無制限な複製を防ぐことが可能である。

【0031】以上、本実施例における半導体記憶媒体によれば、通信系路上での盗聴による情報の不正取得を防止する目的で複数の機器間で暗号通信を行い、転送元機器から転送先機器に情報を渡す際に、「音楽データなどの高付加価値情報を暗号化して転送する」、「上記暗号化に用いた鍵を、別の鍵で暗号化して転送する」と言った二段に鍵を組み合わせた暗号化を行なうことができる。但し、後者の暗号化は、転送先機器では復号不可能な暗号鍵を用いている（鍵を共有していない）ことから、転送先機器で、暗号化された有価値情報を復号し、利用することは不可能となっており、転送元機器に同情報を書き戻した際にのみ利用可能となる。又、高付加価値情報の暗号化に用いる鍵を固定とすることは暗号解読の有力な手掛りを与えることとなり安全上問題があるため、同鍵は、擬似乱数生成器などにより暗号通信が必要となるたびに生成する。転送先機器は、高付加価値情報を暗号化するために生成した鍵を、転送先機器でしか復号できない形で暗号化して高付加価値情報と共に出力してしまうために、鍵管理が容易となり（唯一の鍵のみ管理）、且つ、複数の鍵情報によって記憶容量を圧迫されることがない。

【0032】すなわち、本実施例における半導体記憶媒体によれば、付加価値の高い情報を、複製による不正使用を防ぎながら、例えば PC 向けの大容量磁気記憶装置など、特に情報の複製防止機能を具備していない汎用の情報記憶媒体に保管することが可能である。

【0033】次に、本発明の第 2 の実施例について、図 5 及び図 6 を用いて説明する。図 5 は本発明による情報管理及び移動システムの概略構成図、図 6 は本発明による情報移動システムの第 2 の実施例の動作を示すフローチャートである。図 5 では、本実施例に係る半導体記憶媒体 110a 及び 110b と同媒体制御装置（専用情報処理装置 105、又は汎用情報処理装置 106 及び半導体記憶媒体アクセス手段 107、又は再生装置 108）の概略構成を示す。

【0034】図中、情報 201、対称鍵生成部 202、対称鍵 203、対称鍵暗号処理部 204、非対称鍵暗号処理部 206、データバス 209、暗号処理装置 210、記憶装置 211、I/F 装置 212 及びデータバス 213 は、第 1 の実施例に示したものと同様のものである。

【0035】110a は情報 201 の転送元となる半導体記憶媒体、110b は、情報 201 の転送先となる半導体記憶媒体である。205a はあらかじめ情報転送元半導体記憶媒体 110a の記憶装置 211 に保管された、情報転送先半導体記憶媒体 110b の非対称暗号方式を用いた公開鍵（以下、第 1 の非対称鍵）、205b はあらかじめ情報転送先半導体記憶媒体 110b の記憶装置 211 に保管された、情報転送先半導体記憶媒体 110b の非対称暗号方式を用いた秘密鍵（以下、第 2 の非対称鍵）である。

【0036】501a、501b は専用情報処理装置 105、又は汎用情報処理装置 106 及び半導体記憶媒体アクセス手段 107、又は再生装置 108 との間の情報、制御信号のやり取りを制御するインターフェース装置（以下、I/F 装置）である。

【0037】502 は一方の I/F 装置 501a を介して入力した情報を他方の I/F 装置 501b を介して出力するように制御してなる制御回路である。503a、503b は I/F 装置 501 と制御回路 502 間で情報、制御信号をやり取りするデータバスである。

【0038】次に、図 6 を用いて、情報転送元半導体記憶媒体 110a に保管された情報 201 を専用情報処理装置 105、又は汎用情報処理装置 106 及び半導体記憶媒体アクセス手段 107、又は情報再生装置 108 を介して、情報転送先半導体記憶媒体 110b へ転送する場合の手順を説明する。

【0039】情報転送元半導体記憶媒体 110a に接続された専用情報処理装置 105、又は汎用情報処理装置 106 及び半導体記憶媒体アクセス手段 107、又は情報再生装置 108 による情報 201 の転送要求に応じて、情報転送元半導体記憶媒体 110a 及び情報転送先半導体記憶媒体 110b は以下の動作を行う。

【0040】図 6 において、ステップ 601 で、情報転送元半導体記憶媒体 110a は対称鍵を生成する。即ち、暗号処理装置 210 の機能によって乱数を生成し、生成された乱数は情報 201 を暗号化する対称鍵 203 として用いられる。ステップ 602 で、情報 201 は、暗号処理装置 210 の機能によって、対称鍵 203 を暗号鍵とした対称鍵暗号化を施され、暗号化情報 207 が生成される。上記手順により生成された暗号化情報 207 は、ステップ 603a において、I/F 装置 212 の機能によって、専用情報処理装置 105、又は汎用情報処理装置 106 及び半導体記憶媒体アクセス手段 107、又は再生装置 108 を介して、情報転送先半導体記憶媒体 110b に送信される。

【0041】情報転送先半導体記憶媒体 110b は、ステップ 603b で、暗号化情報 207 を受信し、ステップ 604 で受信した暗号化情報 207 の転送誤りをチェックする。もし転送誤りがあれば、情報転送先半導体記憶媒体 110b は、ステップ 605a で情報転送元半導

第記憶媒体 110a に対し情報再送要求を送信する。情報転送元半導第記憶媒体 110a は、ステップ 605b で、情報再送要求を受信し、ステップ 603a で再度、暗号化情報を送信する。もし転送誤りがなければ、情報転送先半導第記憶媒体 110b は、ステップ 606a で情報転送元半導第記憶媒体 110a に対し情報受信完通知を送信する。

【0042】情報転送元半導第記憶媒体 110a は、ステップ 606b で情報受信完通知を受信し、ステップ 607 で情報 201 の削除動作を行う。この削除動作は、I/F 装置 212 を介して外部からデータアクセスが不可能となることを保証可能であるならば、記憶装置 211 上からの物理的なデータ消去を伴わなくともよい。

【0043】次に、ステップ 608 で、情報転送元半導第記憶媒体 110a は、暗号処理装置 210 の機能によって、対称鍵 203 に第 1 の非対称鍵 205a を暗号鍵とした非対称暗号化を施し、暗号化対称鍵 208 を生成する。上記手順により生成された暗号化対称鍵 208 は、ステップ 609a で、I/F 装置 212 の機能によって、専用情報処理装置 105、又は汎用情報処理装置 106 及び半導体記憶媒体アクセス手段 107、又は情報再生装置 108 を介して、情報転送先半導第記憶媒体 110b に送信される。

【0044】情報転送先半導第記憶媒体 110b は、ステップ 609b で暗号化対称鍵 208 を受信し、ステップ 610 で受信した暗号化対称鍵 208 の転送誤りをチェックする。もし転送誤りがあれば、ステップ 611a で情報転送先半導第記憶媒体 110b は、情報転送元半導第記憶媒体 110a に対し対称鍵再送要求を送信する。情報転送元半導第記憶媒体 110a は、ステップ 611b で対称鍵再送要求を受信し、ステップ 609a に戻り、再度、暗号化対称鍵を送信する。もし転送誤りがなければ、情報転送先半導第記憶媒体 110b は、ステップ 612 で暗号処理装置 210 の機能によって、暗号化対称鍵 208 に第 2 の非対称鍵 205b を暗号鍵とした非対称復号化を施し、対称鍵 203 を生成する。次に、ステップ 613 で情報転送先半導第記憶媒体 110b は、暗号処理装置 210 の機能によって、暗号化情報 207 に対称鍵 203 を暗号鍵とした対称鍵復号化を施し、情報 201 を生成する。

【0045】上記手順によって情報転送元半導第記憶媒体 110a から出力された暗号化情報 207 は、対称鍵 203 がないと正当に復号できない。又、暗号化対称鍵 208 は、第 2 の非対称鍵 205b がないと正当に復号できない。ここで、第 2 の非対称鍵 205b は、情報転送元半導体記憶媒体 110b 固有の鍵データであり、同機器以外ではこれを得ることができない。従って、暗号化情報 207 の転送経路上に存在する、専用情報処理装置 105、又は汎用情報処理装置 106 及び半導体記憶媒体アクセス手段 107、又は再生装置 108 などの機

器においては、暗号化対称鍵 208 を復号して情報 201 を利用することができない。

【0046】又、情報転送元半導第記憶媒体 110a と情報転送先半導第記憶媒体 110b 間のデータ転送過程において、暗号化情報 207 の送出と暗号化対称鍵 208 の送出の間の時点で、情報転送元半導第記憶媒体 110a 内に存在する情報 201 が無効化される（ステップ 607）ため、情報転送元半導第記憶媒体 110a と情報転送先半導第記憶媒体 110b の両方の装置上に、情報 201 が存在する期間が生じない。これにより、暗号化情報 207 の転送完了時点で、情報 203 を保有する権利は情報転送元半導第記憶媒体 110a から情報転送先半導第記憶媒体 110b に移動したとみなすことが可能であり、以降、情報転送元半導第記憶媒体 110a は暗号化対称鍵 208 の送出のみを行うことが可能となる。

【0047】すなわち、情報転送元半導第記憶媒体 110a と情報転送先半導第記憶媒体 110b 間のデータ転送過程の任意の時点において、例えば通信エラーや又は悪意の通信遮断による通信の異常終了が生じたとしても、情報転送元半導第記憶媒体 110a と情報転送先半導第記憶媒体 110b の双方で情報 203 が利用可能となることがないことを保証できる。

【0048】尚、本実施例においては、複数の記憶媒体間でデータを移動する例を示したが、必ずしも複数の記憶媒体間でのデータ移動に限る訳ではなく、記憶媒体 110 と、例えば、専用情報処理装置 105 などの記憶媒体以外の機器間で同様の手順に基づいてデータの移動を実現してもよいし、複数の記憶媒体間に複数の情報再生装置 109 又は専用情報処理装置 105 などを介してデータの移動を実現してもよい。

【0049】又、本実施例においては、暗号化情報の転送（ステップ 603a、603b）又は暗号化対称鍵の転送（ステップ 609a、609b）において、受信された暗号化情報の転送誤りチェック（ステップ 604）又は暗号化対称鍵の転送誤りチェック（ステップ 610）が実行されたとしたが、半導体記憶媒体 110a、110b と、専用情報処理装置 105 などとの間のデータバス 209 の信頼性が高い場合、該転送誤りチェック処理（ステップ 604）又は（ステップ 610）を省略し、暗号化情報受信後すぐに情報受信完転送処理（ステップ 606a、606b）、又は暗号化対称鍵 208 受信すぐに非対称鍵復号化（ステップ 612）の処理を行なってもよい。

【0050】以上、本実施例における半導体記憶媒体によれば、複数の半導体記憶媒体 110a、110b 間で、情報 201 の移動が可能であり、且つ同時に複数の半導体記憶媒体 110a、110b 上で、同一の情報 201 が使用可能となることがないことを保証可能である。すなわち、本実施例における半導体記憶媒体によれ



ば、暗号通信と厳密なトランザクション処理の組み合わせによって、付加価値の高い情報を、複製による不正使用を防ぎながら、記憶媒体間で移動することを可能とした記憶媒体を実現可能である。

【0051】第1及び第2の実施例においては、暗号処理の実装は、暗号処理装置210内の専用のハードウェアによっても、同装置内のCPUとソフトウェア処理によってもよい。又、鍵情報の保管領域、暗号処理に必要なワーク領域は暗号処理装置210内に専用に設けても良いし、記憶装置211を流用しても良い。

【0052】また、第1及び第2の実施例においては、情報201の暗号化に对称鍵暗号方式、同対称鍵203の暗号化に非対称暗号方式を用いる構成を例示したが、必ずしもこの構成に限定するものではなく、情報の暗号化、暗号鍵の暗号化という二段構成を取り、且つ、同暗号鍵を暗号化する鍵を媒体固有に秘密裏に保持することが可能であるならば、用いる暗号方式は、対称鍵暗号方式、非対称鍵暗号方式を任意に組み合わせてよい。

【0053】第1及び第2の実施例で示した半導体記憶媒体110（または110a、110b）は記憶媒体本来の機能である記憶装置211とI/F装置212に加え、暗号処理装置212を具備する。この半導体記憶媒体110は外部装置とのやり取り全てをI/F装置212のみを介して行い、又、例えば記憶装置211、I/F装置212及び暗号処理装置212を同一の半導体ウェハ上に構成することなどにより、上記装置間を接続するデータバス213に外部から直接アクセスすることは困難な構成とする。これにより、半導体記憶媒体110の記憶装置211に記憶された情報201や、暗号処理に必要な鍵情報203、205a、205bに不正にアクセスすることを防止し、耐タンパ性能を高める。

【0054】また、第1及び第2の実施例で示した半導体記憶媒体110の実現形態としては、例えば、フラッシュメモリを記憶装置211とし、暗号処理装置210、I/F装置212を同一の半導体ウェハ上に構成した半導体チップを、例えば切手やクレジットカード程度の大きさのパッケージに封止したものが考えられる。上記形態の半導体記憶媒体110を情報流通媒体とすることで、図1に示したような情報処理システム上で高付加価値情報をユーザが利用する際の利便性を向上させることが可能である。

【0055】又、第1及び第2の実施例では記憶装置211として何らかの半導体記憶装置を用いた半導体記憶媒体について示したが、必ずしも半導体記憶媒体に限定するものではなく、例えば、記憶装置として磁気記憶装置を用いた磁気記憶媒体としても問題はない。この場合、例えば、暗号処理装置210、I/F装置212、磁気記憶装置へのアクセス手段を同一の半導体ウェハ上に構成することで、データバス213への記憶媒体110外からのアクセスを防ぐことが可能である。

【0056】又、上記第1又は第2の実施例においては、半導体記憶媒体110を図2又は図5に示す構成としたが、これを図7に示す構成としてもよい。

【0057】図7は半導体記憶媒体の他の実施例を示す概略構成図であり、第1又は第2の実施例に用いることができる。図において、図2または図5に示す構成要素と同じものには同一の符号を付し、その説明を省略する。図において、212aは、半導体記憶媒体110と外部機器との間で通常のデータ及び制御信号のやり取りを制御するデータインターフェース装置（以下、データI/F装置）である。212bは、半導体記憶媒体110と外部機器との間で安全に交換すべきデータ及び制御信号のやり取りを制御するデータインターフェース装置（以下、セキュアデータI/F装置）である。

【0058】209cは、半導体記憶媒体110と外部機器間で通常のデータ及び制御信号をやり取りするデータバスである。209dは、半導体記憶媒体110と外部機器間で安全に交換すべきデータ及び制御信号をやり取りするセキュアデータバスである。記憶媒体110外部から見えるI/F装置を物理的に複数具備し、例えば、第1の非対称鍵205aや第2の非対称鍵205bの記憶装置211への設定や、ここでは方式の詳細は述べないが記憶媒体110、外部装置間の認証手続きなど、システムの安全上特に重要な情報のやり取りについては、セキュアデータI/F装置212aを介して行う。暗号化情報207の送受信など特に重要ではないものについては、データI/F装置212bを介して行う。

【0059】上記構成によれば、半導体記憶媒体110に物理的に独立した複数のデータI/Fを設けることで、安全上特に重要な情報のやり取りに特化したプロトコルやバス構成を、通常の情報のやり取りとの依存関係なしに定義可能となる。

【0060】以上説明したように、本発明によれば、情報生成者又は情報生成装置と、情報配信装置と、情報を配信する通信回線と、半導体記憶媒体と、該通信回線と接続され該半導体記憶媒体に情報を書き込む端末と、通信回線とは独立した状態で半導体記憶装置に格納されている情報を再生する情報再生装置からなる系において、記憶媒体に格納されている情報を他の情報機器又は記憶媒体で使用することが不可能な形式で出力することが可能な記憶媒体及びそれを用いた情報処理システムを提供することと、記憶媒体に格納されている情報を複製ではなく移動することで、情報の唯一性を保証することが可能である。

【0061】これにより、付加価値の高いデータも安全に半導体記憶媒体で流通させることが可能となり、情報配信サービスなどへの応用が可能となる。

【0062】

【発明の効果】以上説明したように、本発明によれば、

記憶媒体に格納されている情報を他の情報機器又は記憶媒体で使用することが不可能な形式で出力することが可能である。また、記憶媒体に格納されている情報を複製ではなく移動することで、情報の唯一性を保証することが可能である。これにより、付加価値の高いデータも安全に半導体記憶媒体で流通させることが可能となり、情報配信サービスなどへの応用が可能となる。

#### 【図面の簡単な説明】

【図1】本発明を適用することができる情報処理システムの一実施例の概要を示すブロック図である。

【図2】本発明による記憶媒体の第1の実施例を示す構成図である。

【図3】本発明による情報移動システムの記憶媒体からの情報転送機能の第1の実施例を示す図である。

【図4】本発明による情報移動システムの記録媒体への情報転送機能の第1の実施例を示す図である。

【図5】本発明による情報管理及び移動システムの概略構成図である。

【図6】本発明による情報移動システムの第2の実施例の動作を示すフローチャートである。

【図7】半導体記憶媒体の他の実施例を示す概略構成図である。

【図8】図3の情報移動システムの動作を説明するためのフローチャートである。

【図9】従来の複製による不正使用防止システムを示すブロック図である。

【図10】従来の情報移動システムのフローチャートである。

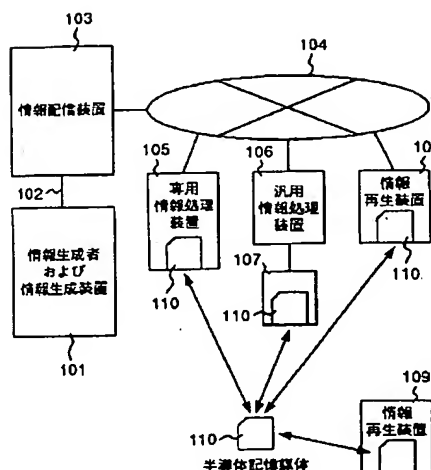
#### 【符号の説明】

101…情報生成者および情報生成装置、102…転送手段、103…情報配信装置、104…通信回線、105

5…専用端末、106…汎用情報処理装置、107…半導体記憶媒体アクセス手段、108…情報再生装置、109…情報再生装置、110…半導体記憶媒体、201…情報、202…対称鍵生成処理、203…対称鍵、204…対称鍵暗号処理、204a…対称鍵暗号化処理、204b…対称鍵復号化処理、205a…第1の非対称鍵、205b…第2の非対称鍵、206…非対称鍵暗号処理部、206a…非対称鍵暗号化処理、206b…非対称鍵復号化処理、207…暗号化情報、208…暗号化対称鍵、209…データベース、209a…暗号化情報、暗号化対称鍵送信、209b…暗号化情報、暗号化対称鍵受信、209c…データベース、209d…セキュアデータベース、210…暗号処理装置、211…記憶装置、212…I/F装置、212a…データI/F装置、212b…セキュアデータI/F装置、501a…I/F装置、501b…I/F装置、502…制御装置、503a…データベース、503b…データベース、601…対称鍵生成処理、602…対称鍵暗号化処理、603a…暗号化情報送信、603b…暗号化情報受信、604…暗号化情報鍵の転送誤りチェック処理、605a…情報再送要求送信、605b…情報再送要求受信、606a…情報受信完送信、606b…情報受信完受信、607…情報の削除処理、608…非対称鍵暗号化処理、609a…暗号化対称鍵送信、609b…暗号化対称鍵受信、610…暗号化対称鍵の転送誤りチェック処理、611a…対称鍵再送要求送信、611b…対称鍵再送要求受信、612…非対称鍵復号化処理、613…対称鍵復号化処理、901…ネットワーク、902…クライアント、903…音楽配信サーバ、910…パーソナルコンピュータ、911…携帯用ヘッドホンステレオ、922…音楽データベース。

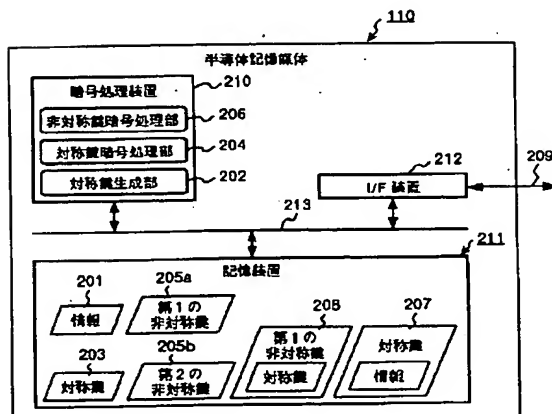
【図1】

図 1



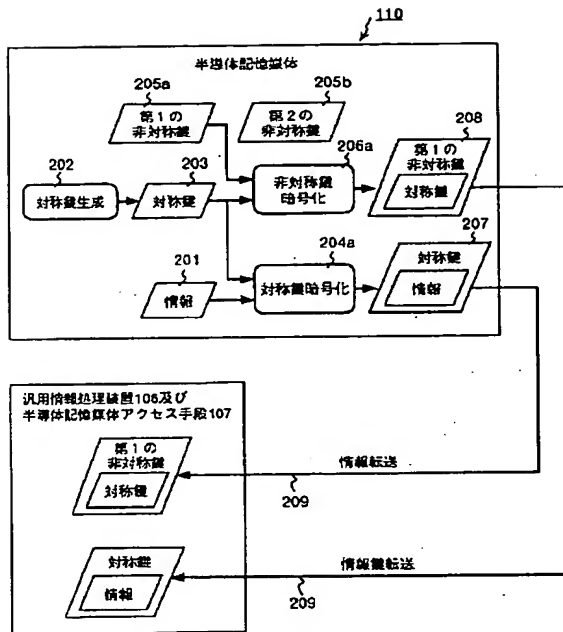
【図2】

図 2



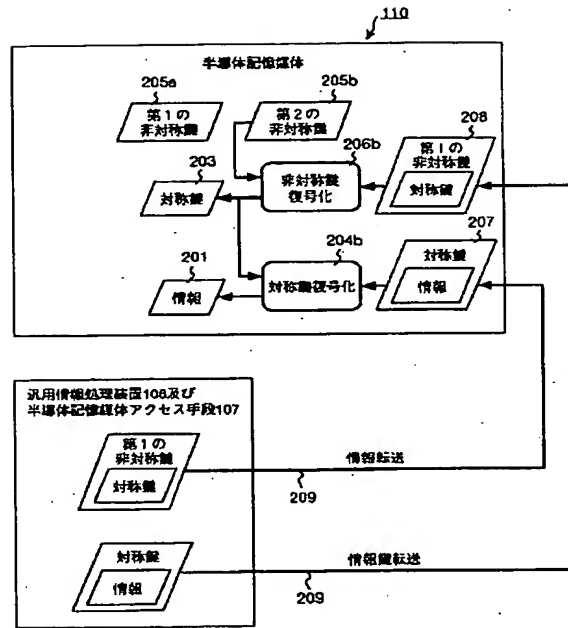
【図3】

図 3



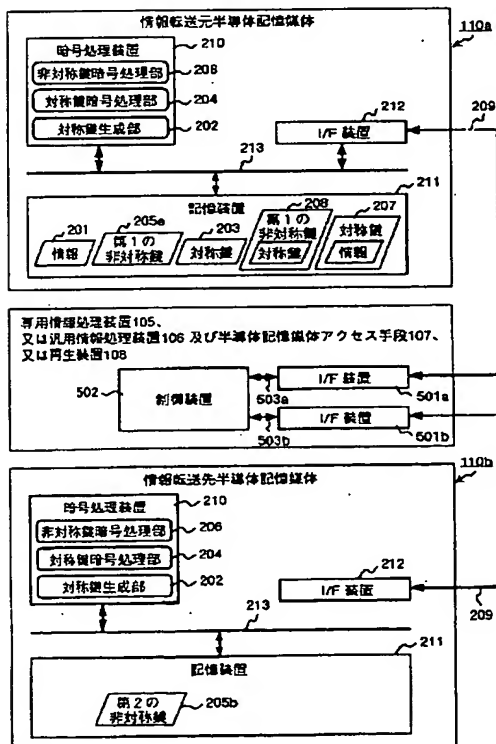
【図4】

図 4



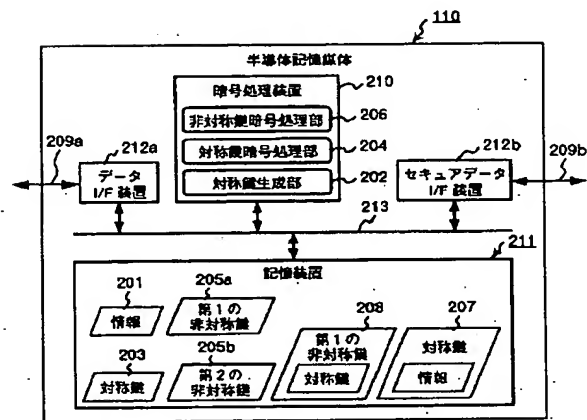
【図5】

図 5



【図7】

図 7

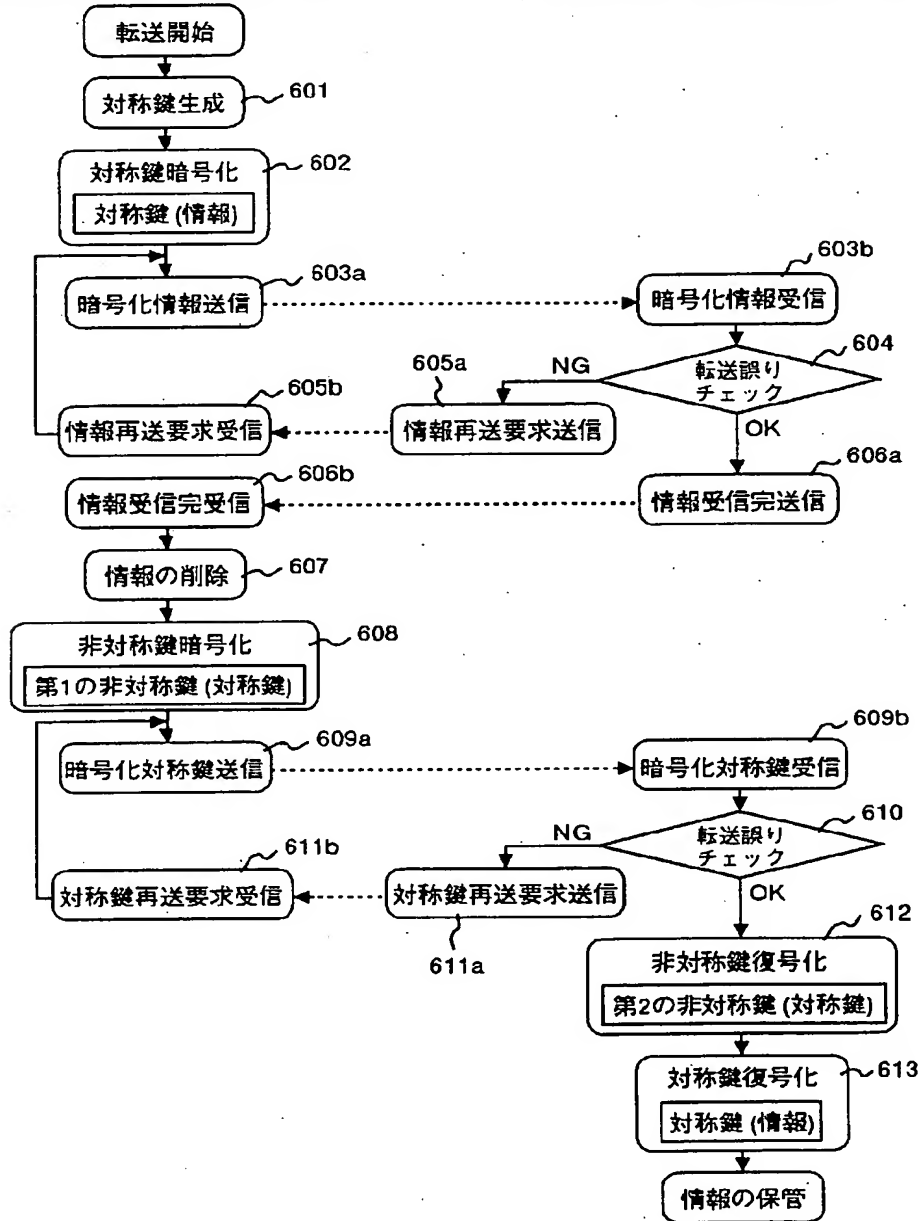


【図6】

図 6

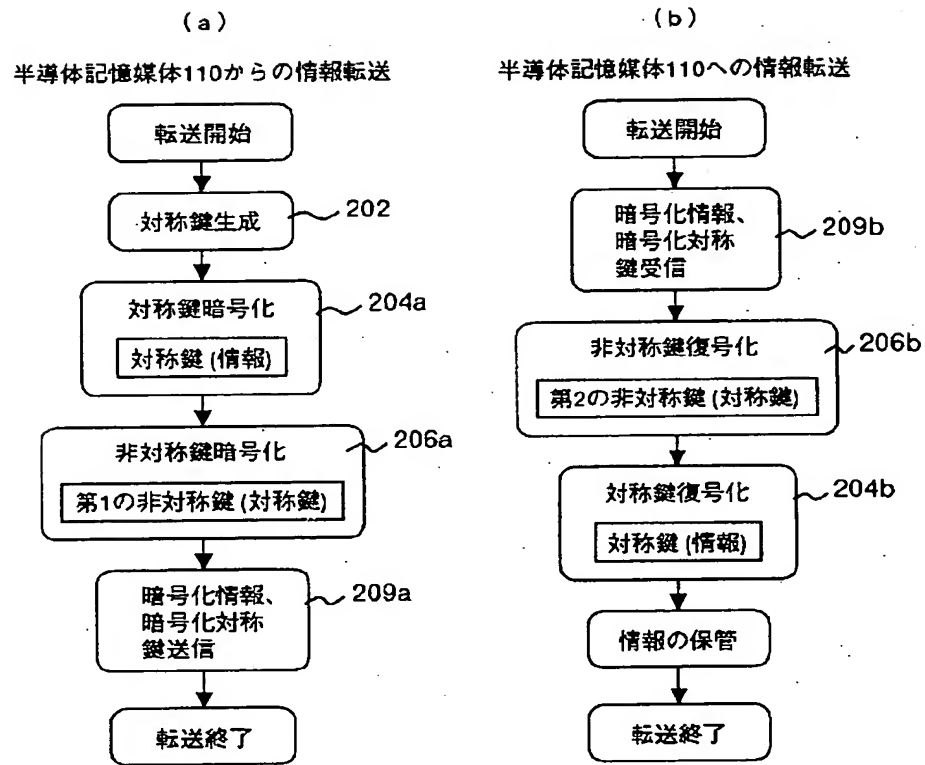
情報転送元半導体記憶媒体 110a

情報転送先半導体記憶媒体 110b



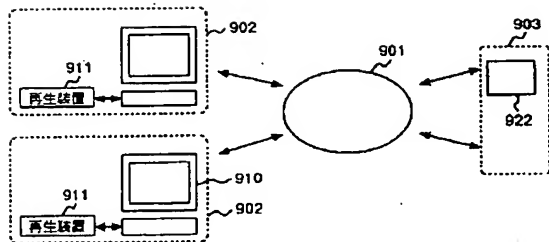
【図8】

図 8



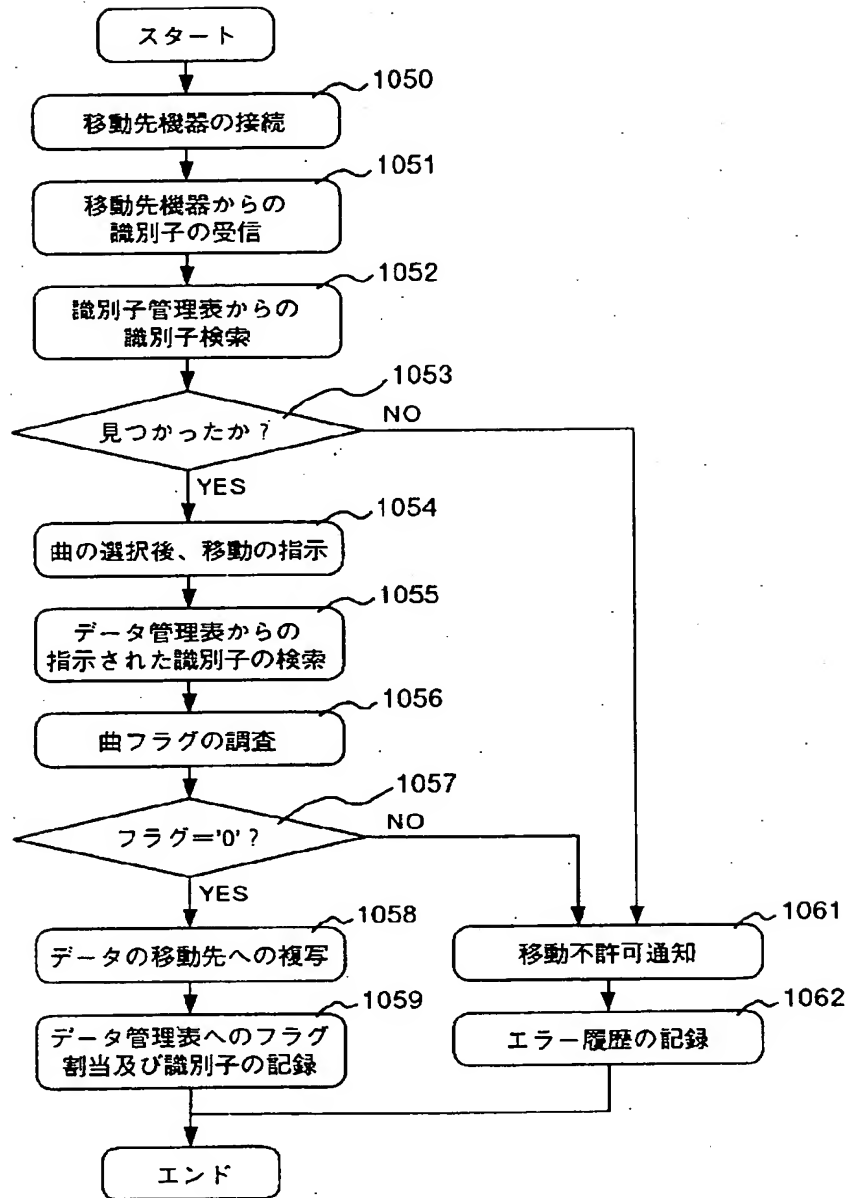
【図9】

図 9



【図 10】

図 10



フロントページの続き

(72) 発明者 朝日 猛  
 神奈川県川崎市麻生区王禅寺1099番地 株  
 式会社日立製作所システム開発研究所内

(72) 発明者 田村 隆之  
 神奈川県川崎市麻生区王禅寺1099番地 株  
 式会社日立製作所システム開発研究所内



(72) 発明者 水島 永雅  
神奈川県川崎市麻生区王禅寺1099番地 株  
式会社日立製作所システム開発研究所内

(72) 発明者 川崎 郁也  
東京都小平市上水本町五丁目20番1号 株  
式会社日立製作所半導体グループ内

(72) 発明者 戸塚 隆  
東京都小平市上水本町五丁目20番1号 株  
式会社日立製作所半導体グループ内

F ターム(参考) 5B017 AA06 BA07 CA16.  
5J104 AA13 AA16 EA04 EA19 EA22  
JA03 NA02 NA35 NA37 NA42